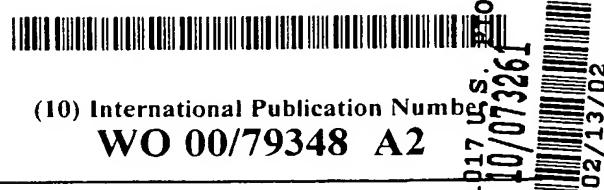


(19) World Intellectual Property Organization
International Bureau(43) International Publication Date
28 December 2000 (28.12.2000)

PCT

(10) International Publication Number
WO 00/79348 A2

(51) International Patent Classification⁷: G04G

(21) International Application Number: PCT/US00/40168

(22) International Filing Date: 8 June 2000 (08.06.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data: 09/338,074 23 June 1999 (23.06.1999) US

(71) Applicant: DATUM, INC. [US/US]: 9975 Toledo Drive, Irvine, CA 92618 (US).

(72) Inventors: ROBINSON, David; 1464 Bullion Circle, San Jose, CA 95120 (US). TYO, David; 4710 Carmonita Lane, Yorba Linda, CA 92886 (US). VAN DER KAAY, Erik, H.: 500 Dahlia Avenue, Corona Del Mar, CA 92625 (US).

(54) International Patent Classification⁷: G04G

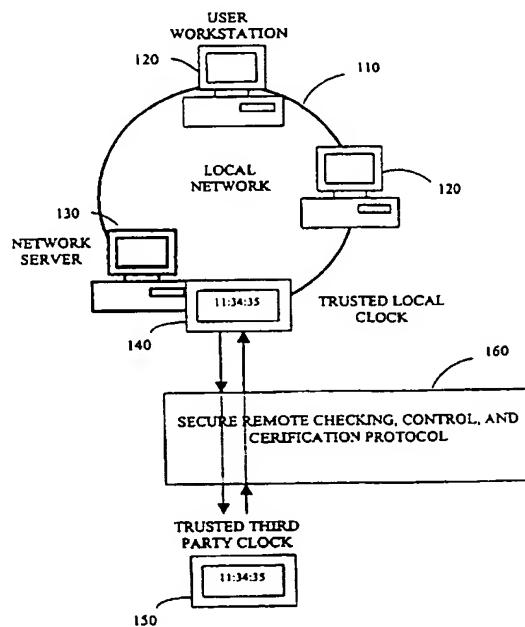
(74) Agent: ALTMAN, Daniel, E.; Knobbe, Martens, Olson And Bear, LLP, 16th floor, 620 Newport Center Drive, Newport Beach, CA 92660 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, CZ (utility model), DE, DE (utility model), DK, DK (utility model), DM, DZ, EE, EE (utility model), ES, FI, FI (utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (utility model), SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR PROVIDING A TRUSTED THIRD PARTY CLOCK AND TRUSTED LOCAL CLOCK



WO 00/79348 A2

(57) Abstract: The present invention involves a system and method of providing a trusted local clock in a computer environment. The local clock is in communication with a certified master clock. The accuracy of the time of the local clock is certified by the master clock. If the local clock departs from a predetermined acceptable error, the master clock updates the local clock. The communication between the master clock and the local clock is a secure, synchronized communication. When the local clock is accurate, the master clock provides certification tokens which the local clock can provide to verify accuracy of its time stamps.



IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

- *Without international search report and to be republished upon receipt of that report.*

This Page
1/2

SYSTEM AND METHOD FOR PROVIDING A TRUSTED THIRD PARTY CLOCK AND TRUSTED LOCAL CLOCK**FIELD OF THE INVENTION**

The present invention relates to electronic time stamp authentication, and in particular, to a system and method for providing remote time certification through the use of a trusted third party clock, a trusted local clock, and
5 a secure synchronization protocol.

BACKGROUND OF THE INVENTION

Electronic Commerce is a rapidly expanding aspect of the economic world and demands the use of Electronic Commerce transactions. Such transactions, however, have outgrown the policies and controls that regulate traditional Paper Commerce. For example, a paper document can be typed, signed in ink, and mailed through the post
10 office. The post office can then affix a time stamp and receipt at the destination. There are long standing legal and accounting policies that authenticate this type of transaction. When an electronic document is sent between two computers, however, it does not leave behind the same degree of tangible evidence. Even if the electronic document is stored in a computer's memory, the contents, signature, and time stamp can be manipulated by anyone with access to the computer.

15 Accounting and legal regulatory bodies are currently developing and mandating Electronic Commerce certification processes to provide reliable authentication for electronic transactions much like those available for paper transactions. Many of the certification processes depend on the creation of a digital signature that authenticates the Who, What, and When of a document.

"When" is a measure of the "time" an event occurred and is a concept easily taken for granted. A world
20 wide system of time standardization is in operation. Each country that is signatory to the Treaty of the Meter maintains a National Timing Laboratory, NTL, which houses the local country's standard time clock. These clocks are kept synchronized to the world standard of time maintained in Paris, France. The world standard for commercial time is "Coordinated Universal Time", UTC. In the United States Congress has mandated official United States "Time" to follow the clock maintained by the National Institute of Standards and Technology (NIST), located in Boulder,
25 Colorado, UTC-NIST. Any time stamp for a transaction that must survive technical, auditing, or legal scrutiny must be made by a clock that is synchronized to UTC-NIST, and the synchronization process must be "traceable".

Throughout this document reference is made to UTC-NIST but the invention described is applicable to operation in any country and with standard time clocks maintained by any country's National Timing Laboratory.

The use of "traceable" clocks in Paper Commerce has been sufficient to provide the "When" of ordinary paper transactions. While there have been numerous cases of falsification of dates on paper documents, the risk to 5 commerce has been relatively small. In the case of Electronic Commerce, however, falsification of dates creates a much greater risk because it is possible to invade computer-directed processes and effect fraud on a very large scale. Such computer crimes frequently involve falsification of electronic time stamps; and for this very reason, protection of the electronic clocks that generate those time stamps from tampering is a high priority in Electronic Commerce.

Current network procedures provide for the synchronization of all workstation clocks in a network. NIST and 10 other agencies provide network time servers that have clocks traceable to UTC-NIST. Client workstations can synchronize their time with the Network Time Servers through a common protocol. The Network Time Protocol (NTP) is commonly used in TCP/IP networks such as the Internet, but other protocols are also used. Unfortunately, once local workstation clocks are synchronized to the Network Time Server, their time may be subject to manipulation regardless of the reliability of the source Network Time Server.

15 Other systems employ the use of certified time that is maintained by a trusted third party's system located outside the local network. The trusted third party system remains synchronized with UTC-NIST through a common protocol. The local network application server then establishes communication with the third party's system whereby a data object (document or transaction record) or a cryptographic hash of the data object is sent to the third party system where a "time stamp" is affixed to the data object, either in clear text or cryptographically embedded. 20 Such a system may be impractical, however, considering the need for external communication for each instance of time stamping and the number of time stamps that are required by the local network.

Another system introduces a local clock into the local network, thus avoiding the problems associated with 25 obtaining time stamps from an outside source. The local clock must be periodically synchronized with a UTC-NIST traceable clock. In order to avoid frequent certification and calibration between the local clock and the UTC-NIST traceable clock, the local clock could be a cesium atomic clock. Cesium atomic clocks are commercially available and their frequency, and hence time, is derived from an atomic phenomena, the energy difference of certain cesium atom

electron orbits. Thus, as long as the cesium atomic clock is operating, it will be accurate enough to satisfy most practical applications. Such clocks only lose one second in 30,000 years of normal operation. For this reason, cesium atomic clocks are termed "Primary Reference Sources." Unfortunately, when used locally, there is still the possibility that the time value in the clock could, through system malfunction or intentional manipulation, be altered to an 5 incorrect value that would not be apparent to a user.

SUMMARY OF THE INVENTION

The present invention addresses the system and method for creating a Trusted Local Clock (TLC), that is remotely checked, controlled and certified using a secure communication method protocol (SRC3) protocol, by a Trusted Third Party Clock, (T3PC). Time stamps generated by such a TLC can be trusted in that the TLC clock cannot 10 be altered by personnel in the local facility. The TLC can be remotely checked for accuracy and stable operation, controlled if necessary to bring it within specified accuracy limits, and certified by the Trusted Third Party to be within some specified tolerance relative to UTC-NIST. The system and method of the present invention overcome the difficulties of prior system as previously discussed and allow a local workstation and application server to provide 15 locally generated trusted time stamps without the cost and difficulty of maintaining a "Primary Reference Source." In particular, the present invention provides secure time stamps through the use of a trusted third party clock system, a trusted local clock system, and a secure synchronization protocol. The present invention can provide the secure time stamps at modest cost, making the invention a valuable asset to Electronic Commerce.

In accordance with one aspect of the invention, the trusted third party clock, T3PC, system includes a clock that has been measured and certified by the NIST or another recognized national time authority to be within a 20 specified time accuracy tolerance relative to UTC-NIST. The T3PC system sends and receives secure data such that it can operate the SRC3 protocol between itself and a TLC.

In accordance with another aspect of the invention, the TLC includes an internal clock that can be remotely checked, controlled and certified by the T3PC using the SRC3 protocol. The TLC system provides the capability of sending and receiving secure data such that it can operate the SRC3 protocol between itself and a T3PC(s). 25 Preferably, the internal clock of the TLC is controlled by the T3PC and is configured to prevent local tampering. In one

embodiment, the T3PC (or master clock) directly controls the TLC's internal clock. The TLC can also be configured to update its own internal clock based on information that can be periodically provided by the T3PC.

In accordance with another aspect of the invention, a T3PC and a TLC can communicate using a secure synchronization protocol. Preferably, the communication is via the Secure Remote Check, Control, and Certify, 5 (SRC3), protocol. This protocol utilizes symmetric key and public key encryption techniques to operate over exposed networks, like the Internet, without being subject to intrusion.

There are five major components to the Secure Remote Check, Control, and Certify protocol. First, using 10 symmetric and public key encryption and authentication technology, the SRC3 protocol establishes a secure communication channel between the T3PC and the TLC. Communication can take place over dial up telephone lines, data networks like TCP/IP, wireless channels, or other types of communication media without restricting the applicability of the SRC3 protocol. Second, the T3PC and TLC exchange secure message data. Third, the protocol 15 allows the T3PC to perform remote checking of the TLC's internal clock. Primarily the T3PC checks the offset of the TLC relative to the T3PC's own internal clock (which has been measured and certified to be within a specified tolerance limit relative to UTC-NIST), but secondarily, TLC current operating status is also communicated to the T3PC. Fourth, based on a measured offset or error of the TLC's internal clock and the TLC's operating status, the 20 T3PC is able to remotely control the TLC to keep its offset within a predefined tolerance limit, and, if necessary, perform operational control functions on the TLC. Fifth, based on the measured TLC offset, the T3PC can certify the accuracy of the TLC. This certification can take place in the form of passing a Time Certificate data object, Tcert, to the TLC. The authenticity of the Time Certificate data object can be verified through the use of a public key signature.

BRIEF DESCRIPTION OF THE FIGURES

These and other features and advantages of the invention will now be described with reference to the drawings of certain preferred embodiments, which are intended to illustrate and not to limit the invention, and in which:

5 Figure 1 is a high-level block diagram of the preferred system of the present invention and illustrates the interaction between the trusted third party clock and the trusted local clock.

Figure 2 is a block diagram of the preferred system of the present invention showing the trusted local clock.

Figure 3 is a block diagram of the preferred system of the present invention showing the trusted third party clock.

10 Figure 4 is a high-level flow diagram of the preferred process of ensuring secure communication through the Secure Remote Check, Calibrate, Certify protocol.

Figure 5 is a flow diagram of the preferred process of exchanging initial session information between the trusted third party clock and the trusted local clock.

15 Figure 6a is a flow diagram of the preferred process of sending a message from the trusted third party clock to the trusted local clock.

Figure 6b is a flow diagram of the preferred process of sending a message from the trusted local clock to the trusted third party clock.

Figure 7 is a flow diagram of the preferred process of performing remote checking of the trusted local clock.

Figure 8 is a flow diagram of the preferred process of performing remote calibrations by the trusted third 20 party clock and certifying the trusted local clock.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention provides a system and method for maintaining a clock, typically installed in an application server within a user's facility, that provides a source of trusted time. In a preferred embodiment, a Trusted Local Clock, (TLC); generates time stamps that are traceable to a National Time Standard. A high-level block diagram of the preferred system is shown in Figure 1. The local network 110 comprises user workstations 120, a local network application server 130, and a TLC 140, which is a module installed within the network application

server. In another embodiment, the TLC could be a separate unit communicating over the local network rather than internal to the application network server. A Trusted Third Party Clock (T3PC) 150 controls the TLC 140 and communicates with the TLC 140 via a secure synchronization protocol 160.

5 **A. Trusted Local Clock**

As shown in Figure 2, the Trusted Local Clock (TLC) is a system that produces time stamps as requested by its host network application server. In the preferred embodiment, the TLC contains a Local Clock 210, a Time Stamp Encryption Engine 220, a Key Management system 230, a Secure Remote Checking, Control, and Certification Encryption Engine 240, a Processor 250, a Bus Communication Port 260, an SRC3 Communication Port 270, and an 10 optional Local Frequency and Time Reference 280.

The Local Clock 210 contains a Frequency Source 211 such as a voltage controlled quartz oscillator. In other embodiments, an external quartz, rubidium, or cesium oscillator could be used. Associated with the Frequency Source 211 is a Counter 212 that counts the cycles of the Frequency Source 211. The frequency of the Frequency Source 211 and data format of the Counter 212 are such that the counter output is a time stamp, T_n . Connected to 15 the Counter 212 is an Input/Output SET/READ Function 213 that can be used in a supervisory or setup mode of operation to SET the correct current time into the Counter 212, or by the SRC3 protocol to READ current time. The Counter 212 can be triggered at instant n by a Time Stamp Request to latch the current time stamp, T_n , into the Output Time Stamp Circuit 214. The Frequency Source 211 is also associated with an Input/Output STEER Function 215 and Control and Measurement Circuits 216 used to measure and adjust the frequency of the Frequency Source 20 211. The Input/Output STEER Function 215 fine tunes the frequency of the Frequency Source 211 typically by modifying the divisor for the counters to modify the frequency. Alternatively, the control voltage to a voltage controlled quartz oscillator may be used to vary frequency, or if an external rubidium or cesium oscillator is used, the 'C' field oscillator control may be modified.

The frequency Source 211 and Control and Measurement Circuits 216 are constrained in such a way that 25 the maximum STEER change will not allow the frequency and subsequent counter integration to alter the clock time by more than the specified accuracy tolerance over a period of several certification intervals. This means a single

erroneous STEER command cannot invalidate the time stamp, T_n . The Control and Measurement Circuits 216 are also able to READ the Counter 212 and pass current time through the SRC3 protocol.

The Time Stamp Encryption Engine 220 manages the encryption/decryption of time stamp requests. The Time Stamp Encryption Engine 220 receives a time stamp request containing data, H_1 , which is typically a message digest or a hash of a message to be time stamped. The Time Stamp Encryption Engine 220 then sends a Time Stamp Request to the Local Clock 210. The Local Clock latches the current time, T_n , in the Output Time Stamp Circuit 214 and passes it to the Time Stamp Encryption Engine 220. The Time Stamp Encryption Engine 220 catenates the request data H_1 with the time stamp T_n and some verification data, ID, that can be used to identify the time stamping transaction for later verification. This verification data can comprise an assigned clock name, serial number, transaction counter, or other data to be established. A new message digest or hash, H_2 , is created from the catenated data $H_1 + ID + T_n$. The new digest or hash H_2 is signed through Public Key Cryptography (to be discussed below) with the TLC's private signing key, $K_{private}$. H_1 , ID, T_n , H_2 , and the signature are returned to the requesting application through the Bus Communication Port 260.

The TLC's public key, which corresponds to the TLC's private key, is made publicly accessible. A receiving application can verify the authenticity of the time stamped, signed message with the TLC's public key using algorithms that are well known in the art. In particular, the receiving application attempts to decrypt the signature using the TLC's public key to yield H_{2A} . The receiving application also rehashes $H_1 + ID + T_n$ to yield H_{2B} . If the decrypted signature, H_{2A} , matches the hash H_{2B} , then the authenticity of the signature and the validity of H_1 , ID, and T_n are established.

The Key Management System 230 manages and stores all of the TLC's keys. The TLC's keys comprise the private key, $K_{private}$, used by the Time Stamp Encryption Engine 220, as well as a secret session key, K_s , used by the SRC3 Encryption Engine.

The SRC3 Protocol Encryption Engine 240 supports communication with a T3PC through the SRC3 Protocol 160 by encrypting and decrypting Management and Time Data needed to regulate and control the TLC. The Secure 25 Synchronization Protocol Encryption Engine 240 encrypts/decrypts data through Symmetric Key Encryption (to be discussed below) using the secret session key, K_s . The SRC3 Protocol Data is sent through the SRC3 Protocol Port

270, which can be a telephone dial up, network, or other communication channel without restricting the operation of the device.

The Processor 250 controls the overall operation of the TLC 140. An optional feature incorporates the use of a Local Frequency and Time Reference 280. Local information from sources such as Global Position System, Loran, 5 Telecommunications carriers such as E1/T1 lines, etc. can be used to provide a comparison between the frequency of the Frequency Source 211 and the time contained in the Counter 212, and the external reference source. This comparison provides an indication of the 'health' of the local clock and can be used to provide operational status information through the SRC3 Protocol to the T3PC.

B. Trusted Third Party Clock

10 The Trusted Third Party Clock (T3PC) 150, as illustrated in Figure 3, is a system that contains a local master clock and performs checking, control, and certification of remote clocks. In the preferred embodiment, the T3PC 150 comprises a Master Clock 310, a Clock Controller 320, a Key Vault & Management System 330, an Encryption Engine 340, a Processor 350, a Communication Port 360, and Calibration Log 370. An optional Local Frequency and Time Reference 380 can also be incorporated into the T3PC 150.

15 The Master Clock 310 includes a Frequency Source 311. High quality quartz oscillators, rubidium oscillators, or cesium oscillators; could be used for this function. Associated with the Frequency Source 311 is a Counter 312 that counts the cycles of the Frequency Source 311. The frequency of the Frequency Source 311 and data format of the Counter 312 are such that the counter output is a time stamp, T_n . Connected to the Counter 312 is an Input/Output SET/READ Function 313 that can be used in a supervisory or setup mode of operation to SET the 20 correct current time into the Counter 312, or by operation of the processor to READ current time. The Counter 312 can be triggered at instant n by a Time Stamp Request to latch the current time stamp, T_n into the Output Time Stamp Circuit 314. The Frequency Source 311 is also associated with an Input/Output STEER Function 315 and Control and Measurement Circuits 316 used to measure and adjust the frequency of the Frequency Source 311. The Input/Output STEER Function 315 fine tunes the frequency of the Frequency Source 311 typically by altering the control voltage to 25 a voltage controlled quartz oscillator, or if an external rubidium or cesium oscillator is used, the 'C' field oscillator control. The Frequency Source 311 and Control and Measurement Circuits 316 are constrained in such a way that

the maximum STEER change will not allow the frequency and subsequent counter integration to alter the clock time by more than the specified accuracy tolerance over a period of several certification intervals. This means a single erroneous STEER command cannot invalidate the time stamp, T_n . The Control and Measurement Circuits 316 are also able to READ the Counter 312 and compare Time Stamps, T_n with time data received from remote clocks via the 5 SRC3 protocol. The Encryption Engine 320 manages the encryption/decryption of various communication protocols, including protocols for communication with a national time laboratory clock and Trusted Local Clocks 140 using the secure synchronization protocol 160. The Key Vault & Management System 330 manages and stores all of the T3PC's encryption keys. The Key Vault & Management System houses the T3PC's private key as well as a set of TLC secret session keys that are assigned to TLCs as requested. The Key Vault & Management System 330 also 10 keeps track of the TLCs to which secret session keys are assigned.

The Encryption Engine 340 supports the secure synchronization protocol 160 by symmetrically encrypting and decrypting the Management & Time Data needed to communicate with the TLCs (Symmetric Key Encryption will be discussed below). The Encryption Engine 340 uses a different secret session key for each TLC to encrypt/decrypt data.

15 The Processor 350 controls the overall operation of the T3PC. Data input/output is sent via Communication Ports 360. Preferably, the Communication Port 360 utilizes TCP/IP internetworking over public Internet or private networks or similar protocols over the Public Telephone System Network, PTSN. In other embodiments, other communication methods can be used.

20 The Calibration Log 370 contains a listing of time certified TLCs. The information preferably includes the TLC's identity as well as a time stamp signifying when the entry was made. Outside entities have remote access to the Calibration Log 370 to verify that the time stamp they received was sent from a "certified" TLC.

C. SRC3 Protocol

25 The Secure Synchronization Protocol 160 allows the T3PC 150 to check, control, and certify the TLC's 140 internal clock from a remote location using encryption technology to maintain a secure communication. In the preferred embodiment of the present invention, the Secure Synchronization Protocol 160 comprises the Secure Remote Checking, Control, and Certification protocol (SRC3). The Trusted Local Clock's internal Local Clock 210 is

controlled solely by the T3PC 150 using secure encryption technology via the SRC3 160. The Local Clock 210 can not be SET locally, except through special supervisory modes. In this manner, the present system prevents falsification of time stamps by "hackers" either attacking through the communication channel or in collusion with someone from within the user's premises. Yet, the SRC3 protocol allows the TLC to provide, within the user's

5 premises, a means of generating certified time stamps that can be used in Electronic Commerce.

1. Encryption

In the preferred embodiment, the SRC3 transfers configuration status, time, frequency, and update information between the T3PC and the TLC. Commercially available encryption technology provides for high security communication between the T3PC and the TLC. SRC3 preferably uses both Symmetric Key Encryption and Public Key

10 Cryptography.

Symmetric Key encryption is the technique whereby both parties to a desired secure transaction, A and B, share a common secret key, K. A encrypts a message with K and then sends the encrypted message to B. B receives the encrypted message and decrypts it using K.

In Public Key Cryptography, A and B each have two related keys, a private key and a public key. The public key is known to everyone. A encrypts a message to B with B's public key and then sends the encrypted message to B. B receives the encrypted message and decrypts it with B's private key. In a variation, known as "signing," A encrypts a hash of the message with A's private key. B, or any other party, can verify that the message originated from A and has not been altered by decrypting the encrypted hash of the message with A's public key. Public Key Cryptography has the advantage of not requiring the transfer of secret keys between participants. It is widely used in various forms of Electronic Commerce communications and is known as Public Key Infrastructure (PKI). The disadvantage of PKI is that it requires large amounts of processing power and slows down the host computer.

20

Hybrid systems send the text of a message encrypted with symmetric key codes and then encrypt the symmetric secret key with public key technology. This approach utilizes the speed advantages of symmetric key encryption and also solves the problem of sharing secret keys.

25 2. Communication Protocol Components

In a preferred embodiment, SRC3 comprises five major communication protocol components as shown in Figure 4. First, the Initiate Secure Message Transfer 410 is a one time interchange where the T3PC passes a new secret session key, K_s , to the TLC. Second, the Secured Message Transfers 420 allows the T3PC and the TLC to pass secure data between them using K_s . Third, the Time Transfer and Comparison 430 computes the offset of the 5 TLC clock relative to the T3PC when necessary. This component will typically be executed twice in an SRC3 protocol exchange. Fourth, the Control 440 permits the T3PC to make adjustments to the TLC's Local Clock 216. And, fifth, Certification 450 is used to pass a Time Certification, T_{cert} from the T3PC to the TLC.

a. Initiate Secure Message Transfer

The Initiate Secure Message Transfer 410 allows the T3PC to securely exchange a secret session key with 10 the TLC. This secret session key will be used for most future communications between the T3PC and the TLC. As shown in Figure 5, the T3PC first concatenates message data, G_1 , and a new secret session key, K_s , from its key vault 15 creating a new message, G_2 , at a step 501. Next, the T3PC encrypts the message G_2 using the targeted TLC's public key, $K_{TLCpublic}$, generating encrypted message, $K_{TLCpublic}(G_2)$ at a step 502. This ensures that only the target TLC will be able to recover the session key, K_s . At a next step 503, the T3PC "signs" the message by encrypting a hash of 20 $K_{TLCpublic}(G_2)$ with the T3PC's private key, $K_{T3PCprivate}$, generating the signature $K_{T3PCprivate}(K_{TLCpublic}(G_2))$. The use of a "signature" will help to authenticate the interchange allowing the recipient to verify the sender by decrypting the message using the sender's public key. At a next step 504, the T3PC sends the encrypted message $K_{TLCpublic}(G_2)$ and 25 signature, $K_{T3PCprivate}(K_{TLCpublic}(G_2))$, to the TLC.

The TLC receives the encrypted message $K_{TLCpublic}(G_2)$ and signature, $K_{T3PCprivate}(K_{TLCpublic}(G_2))$ at a step 505. At 20 a step 506, the TLC attempts to decrypt the signature using the T3PC's public key, $K_{T3PCpublic}$, at a step 506. If the signature decodes properly and matches a hash of the encrypted message $K_{TLCpublic}(G_2)$, the TLC will know that the encrypted message was sent by the T3PC. If the signature does not match the encrypted message, the TLC will send an error message to the T3PC. At a step 507, the TLC decodes the message, $K_{TLCpublic}(G_2)$, using the TLC's private key, 25 $K_{TLCprivate}$, generating message G_2 . The TLC then extracts the message data, G_1 , and the secret session key, K_s , from message G_2 at a step 508. Next, the TLC concatenates the original message data, G_1 , with its own firmware version information, F_1 , or other TLC identifying data that might be required by the T3PC, creating message $G_3 = G_1 + F_1$ at a

step 509. The TLC encrypts message G_3 with the secret session key, K_a , generating encrypted message $K_a(G_3)$ at a step 510. Next, the TLC "signs" the encrypted message $K_a(G_3)$ with it's private key, $K_{TLCprivate}$, generating the signature, $K_{TLCprivate}(K_a(G_3))$ at a step 511. Finally, the TLC sends the encrypted message $K_a(G_3)$ and signature $K_{TLCprivate}(K_a(G_3))$ to the T3PC at a step 512.

5 At a step 513, the T3PC receives the encrypted message $K_a(G_3)$ and signature $K_{TLCprivate}(K_a(G_3))$. At a step 514, the T3PC attempts to decrypt the signature using the TLC's public key, $K_{TLCpublic}$ generating message. If the signature decodes properly and matches a hash of the encrypted message $K_a(G_3)$, the T3PC will know that the encrypted message was sent by the TLC. At a step 515, the T3PC decrypts the encrypted message $K_a(G_3)$ using the secret session key, K_a generating message G_3 . Finally, at a step 516, the T3PC extracts the message data, G_2 , and 10 the firmware version information, F_1 , from message G_3 . At this point, the secret session key, K_a , has been transferred and verified, and the T3PC and the TLC are ready to communicate.

b. Secured Message Transfers

The Secured Message Transfer 420 allows operation data to be transferred between the T3PC and the TLC through a series of requests and responses. These transactions are encrypted and protected using the secret session key, K_a . Preferably, the message and request/response data comprises the following: message number to synchronize each message with its response, message type to identify the type of information being transferred, message body to pass information associated with the request/response data, and internal time. The message number and/or internal time are included to make each message unique and 'alive' for only a short interval as determined by processing algorithms. This feature is a common method of preventing "replay" attacks with previously intercepted messages. 15 The TLC maintains its current certification status/information, including a history of recent interactions with all T3PCs as well as statistics of time and frequency information, and is ready to send it to the T3PC upon request.

20 Both the TLC and the T3PC can send a message to the other party. Figure 6a illustrates the preferred Secured Message Transfer 420 where the T3PC sends a message to the TLC. First, the T3PC creates the necessary message data, D at a step 601. Second, the T3PC encrypts the message data D using the secret session key, K_a , generating encrypted message, $K_a(D)$ at a step 602. Then, the T3PC sends the encrypted message to the TLC at a 25 step 603. The TLC receives the encrypted message, $K_a(D)$ at a step 604. Next, the TLC decrypts the message using

the secret session key, K_a at a step 605, generating message D. Finally, the TLC extracts necessary information from message D at a step 606. Figure 6b shows a similar exchange with the TLC initiating the communication.

In other embodiments, the Secured Message Transfer 420 also includes having the sending party "sign" the message. This would add another level of security to the message.

5

c. Time Transfer and Comparison

The Time Transfer and Comparison 430 is a 'checking' process which allows the T3PC to measure accurately the offset of the TLC's local clock to the time maintained in the T3PC Master. In the preferred embodiment, the T3PC sends the initial time data to the TLC unencrypted, but signed by the session key. Sending the time data unencrypted minimizes transmission latency. To avoid security risk, the TLC insures that no significant 10 delays are accepted and calibration will only be achieved after a correct time transfer.

As illustrated in Figure 7, the T3PC preferably sends unencrypted, signed time data at a known time, x, preferably saving the time stamp, x, in an array of send time information, $T_s[i] = x$ at a step 702. After receiving the time data at a step 703, the TLC records the time when it received the time data as time stamp, y, at a step 704. The TLC then echoes the received time data, y, back to the T3PC at a step 705 along with a new echo time stamp, v, 15 for the send time from the TLC. When the T3PC receives this time data back from the TLC at a step 706, the T3PC records the time it received the echoed time data as time stamp, z, preferably in an array of final return time information $T_r[i] = z$ at a step 707. The T3PC also retains the received time stamp, y, in an array of received time information, $T_r[i] = y$, and the echo time in an echo time array $T_e[i] = v$.

The T3PC sends and receives an echo for a sufficient number of messages (i+1, i+2, i+3, etc.), as 20 indicated by repeating the steps 702-707 using the 'while' loop steps 701, 708. The number of 'sufficient' messages is determined by the degree of accuracy required and timing errors in the communication channel. The T3PC will be able to require a 'number of sufficient messages' such that the average of all measurements will meet accuracy requirements. The T3PC is ready to calculate the time transfer after a sufficient number of messages.

In the preferred embodiment, the T3PC first uses the send times and the return times to determine the round 25 trip time at a step 713:

$$\text{Round Trip Time} = (T_r[i] - T_s[i]) + (T_e[i] - T_r[i]) \cdot k \text{ (where } k \text{ accounts for known hardware delays)}$$

The multiple messages are used to reduce the time measurement noise. Next, the T3PC calculates the One Time Direction Delay, $T_{1\text{way}}[i]$ at a step 714 which is assumed to be $\frac{1}{2}$ of the Round Trip Time, One Time Direction Delay = $T_{1\text{way}}[i] = \text{Round Trip Time} / 2$

Finally, the T3PC calculates the Estimated Time Error of the TLC at a step 715.

5 Estimated Time Error = $T_{1\text{way}}[i] \cdot (T_r[i] - T_s[i])$.

Knowing the current Estimated Time Error and interval between this measurement and a previous measurement, the T3PC can also determine the frequency error of the TLC Frequency Source 211. The T3PC can then use the gathered data to determine whether adjustments should be made to the TLC. In other embodiments, the TLC could initiate the time measurement process.

10 **d. Control**

The Control 440 allows the T3PC to control the TLC's local clock. As mentioned above, in one embodiment, control entails merely providing update information for the TLC, by which the TLC updates itself. In another embodiment, the T3PC sends update commands to the TLC.

15 As illustrated in Figure 8, based on Estimated Time Error and frequency error measurements performed by the T3PC, the T3PC will Send Corrections to TLC at a step 801. The TLC receives the corrections at a step 803. At the TLC, Control and Measurement Circuits 216 will be used to perform appropriate STEER commands at a step 804.

20 **e. Certification**

After any corrective actions have been performed, another Time Transfer and Comparison 430 operation is performed. Assuming the TLC is still within specified accuracy limits, the T3PC passes a Tcert to the TLC, and the 20 T3PC logs the time as well as the TLC's identity into a calibration log at a step 805. Outside entities have remote access to the T3PC's calibration log to verify that the sender of the time stamps is certified. Upon receipt of the calibration token, the TLC is allowed to provide "certified" time stamps at a step 806.

In the preferred embodiment, the Tcert itself comprises:

25 T3PC Clock ID
TLC Clock ID
Time Stamps Issued
TLC Signature Parameters and Signature
Tcert Time (from T3PC)
30 Tolerance

TLC Clock Offset
Tcert Expiration Time
T3PC Signature Parameters and Signature

5 In other embodiments the data may differ, but typically the T3PC should provide a signed certification that the TLC local clock is within pre-established accuracy limits relative to the T3PC Master Clock (which in turn is certified relative to a National Time Standard).

WHAT IS CLAIMED IS:

1. A system for providing trusted time comprising:
 - a master clock system;
 - 5 a trusted local clock system in communication with said master clock system; and
 - a secure communication between said master clock system and said trusted local clock system, wherein said master clock system checks the local clock time and provides information to said local clock system to update said local clock system based upon said check.
- 10 2. The system of Claim 1, wherein said master clock system comprises a certified clock.
3. The system of Claim 2, wherein said certified clock is certified to a national time authority.
- 15 4. The system of Claim 1, wherein said master clock system and said local clock system establish a synchronized communication.
5. The system of Claim 1, wherein said master system clock checks the time maintained by said trusted local clock system by analyzing send and receive times for time data transferred between the master clock system and local clock system.
- 15 6. The system of Claim 1, wherein said master clock system further comprises:
 - a frequency source;
 - a key management system;
 - a communications port; and
 - 20 an encryption engine in communication with said key management system.
7. The system of Claim 6, wherein said master clock further comprises calibration log.
8. The system of Claim 7 wherein said local clock system interacts with local references.
9. The system of Claim 7, wherein said key management system comprises a key vault containing several keys.
- 25 10. The system of Claim 1 wherein said trusted local clock system further comprises:
 - a frequency source;
 - a local key management system;

a communications port; and

a cryptographic engine.

11. The system of Claim 1, wherein said master clock system is remote from said trusted local clock system.

5 12. A method for controlling a remote clock with a master clock, said method comprising the steps of:
providing a trusted local clock system and a master clock system;
obtaining time data from said local clock with said master clock and comparing said data at said master clock system using a secure communication; and
updating said trusted local clock system with said master clock system.

10 13. The method of Claim 12, wherein said master clock system comprises a certified master clock system.

14. The method of Claim 13, wherein said certified master clock system comprises:
a certified master clock;
a key management system;
a communications port; and
a cryptographic engine in communication with said key management system.

15 15. The method of Claim 13 wherein said certified master clock comprises:
a frequency source; and
an adjustable counter which counts cycles of said frequency source and outputs a time.

20 16. The method of Claim 14, wherein said key management system maintains several keys.

17. The method of Claim 12, wherein said trusted local clock system comprises:
a local clock;
a local key management system;
a communications port; and
a cryptographic engine.

25 18. The method of Claim 17, wherein said local clock further comprises:

a frequency source; and
an adjustable counter which counts cycles of said frequency source and outputs a time format.

19. A method of providing remote certification of time comprising steps of:
 - establishing a remote communications between a local clock and a certified clock;
 - exchanging initial session information between said certified clock and said local clock;
 - monitoring said local clock with said certified clock;
 - updating said local clock with said certified clock; and
 - certifying accuracy of said local clock.
20. The method of Claim 19, wherein said step of exchanging further comprises exchanging at least one session key between said certified clock and said local clock.
21. The method of Claim 19, wherein said step of exchanging comprises exchanging public keys.
22. The method of Claim 19, wherein said step of monitoring further comprises collecting time information from said local clock.
23. The method of Claim 19, wherein said step of monitoring further comprises comparing time information collected from said local clock with certified time of said master clock.
24. The method of Claim 19, wherein said step of updating further comprises determining whether adjustment of said local clock is necessary.
25. The method of Claim 19, wherein said step of certifying the accuracy of the local clock comprises passing a calibration certificate to said local clock.
26. The method of Claim 19, wherein said step of certifying further comprises adding said local clock to a calibration log of said certified clock.
27. A system for providing trusted time comprising:
 - a master clock system comprising a master clock;
 - a trusted local clock system in communication with said master clock system, said trusted local clock system comprising a trusted local clock having a local clock time; and

a secure communication between said master clock system and said trusted local clock system, wherein said master clock system is configured to check the local clock time and certify accuracy of the trusted local clock through said secure communication.

28. The system of Claim 27, wherein said master clock system is configured to update the local clock 5 time through said secure communication.

29. The system of Claim 28, wherein said master clock is a certified clock.

30. The system of Claim 29, wherein said master clock is certified to a national time authority.

31. The system of Claim 27, wherein said master clock system and said trusted local clock system establish a synchronized communication.

10 32. The system of Claim 27, wherein said master clock system checks the local clock time by analyzing send and receive times for data transferred between said master clock system and said trusted local clock system.

33. The system of Claim 27, wherein said master clock system further comprises:

a key management system;

15 a communications port; and

an encryption engine in communication with said key management system.

34. The system of Claim 33, wherein said master clock system further comprises a calibration log.

35. The system of Claim 34, wherein said trusted local clock system interacts with local time references.

20 36. The system of Claim 33, wherein said key management system comprises a key vault containing several keys.

37. The system of Claim 27 wherein said trusted local clock system further comprises:

a local key management system;

a communications port; and

25 a cryptographic engine.

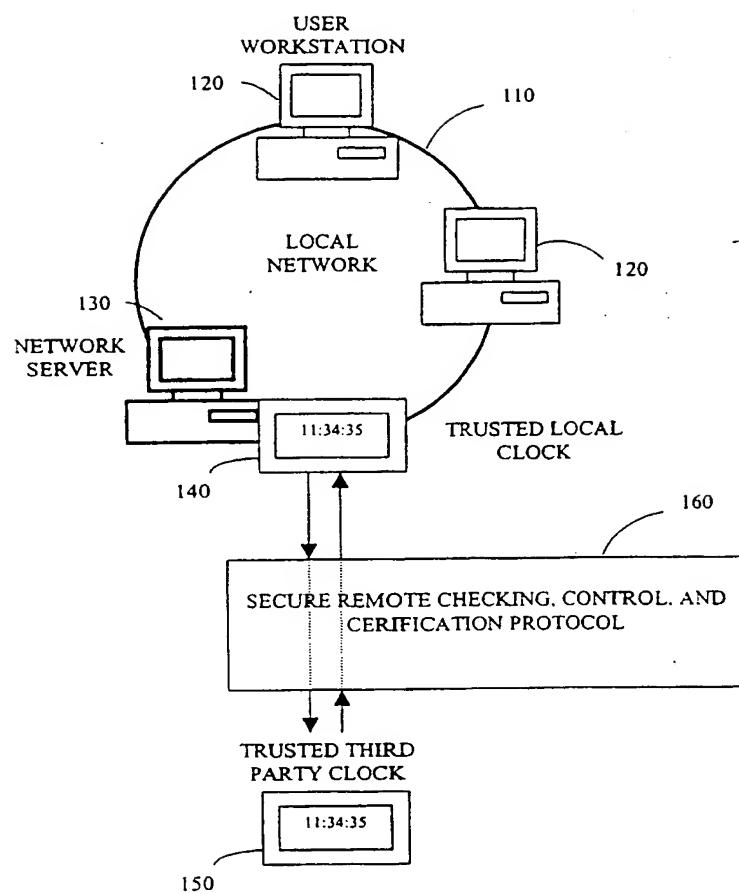
Figure 1

Figure 2

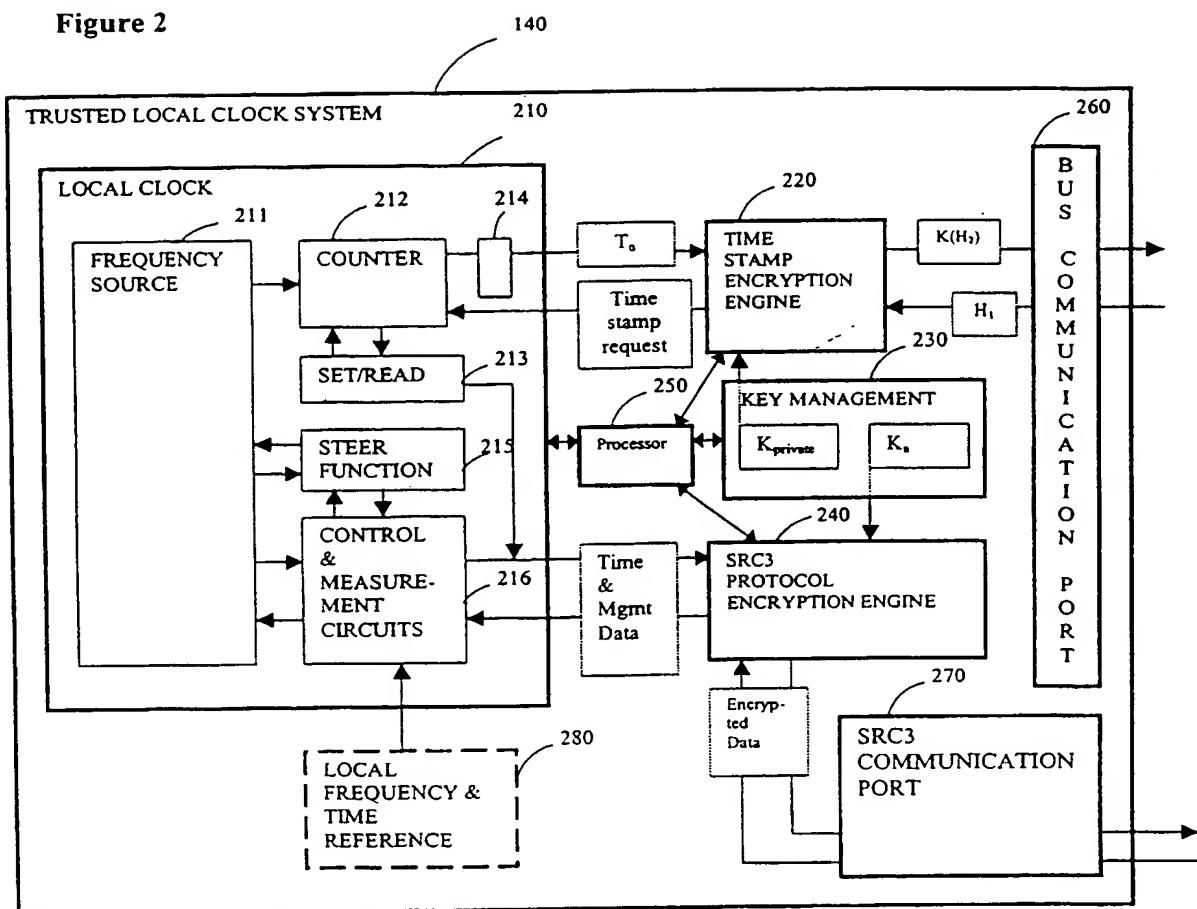


Figure 3

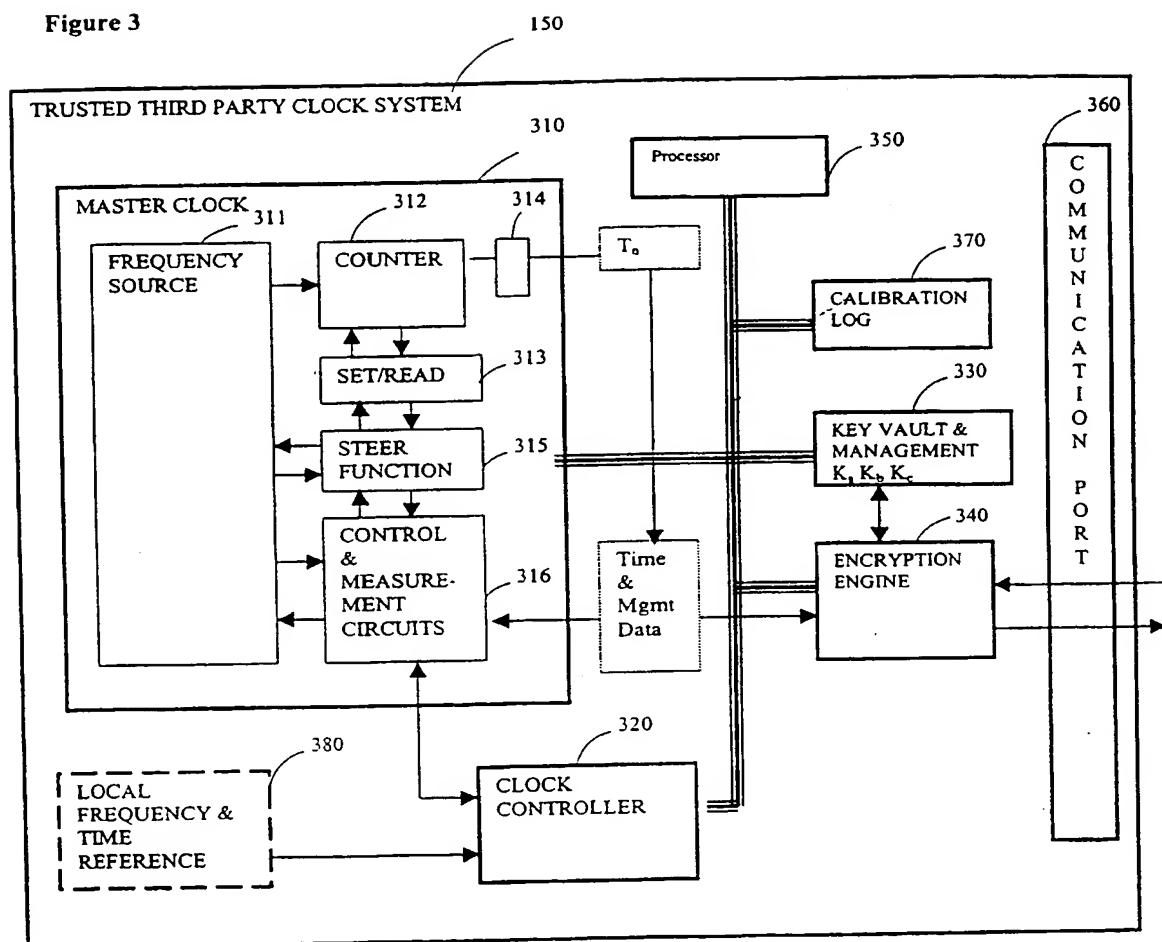


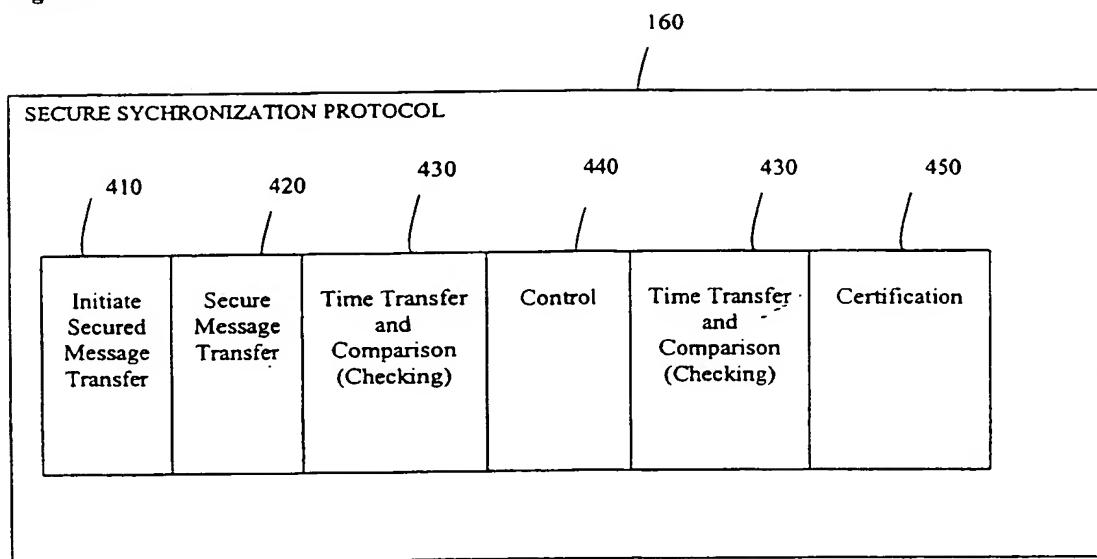
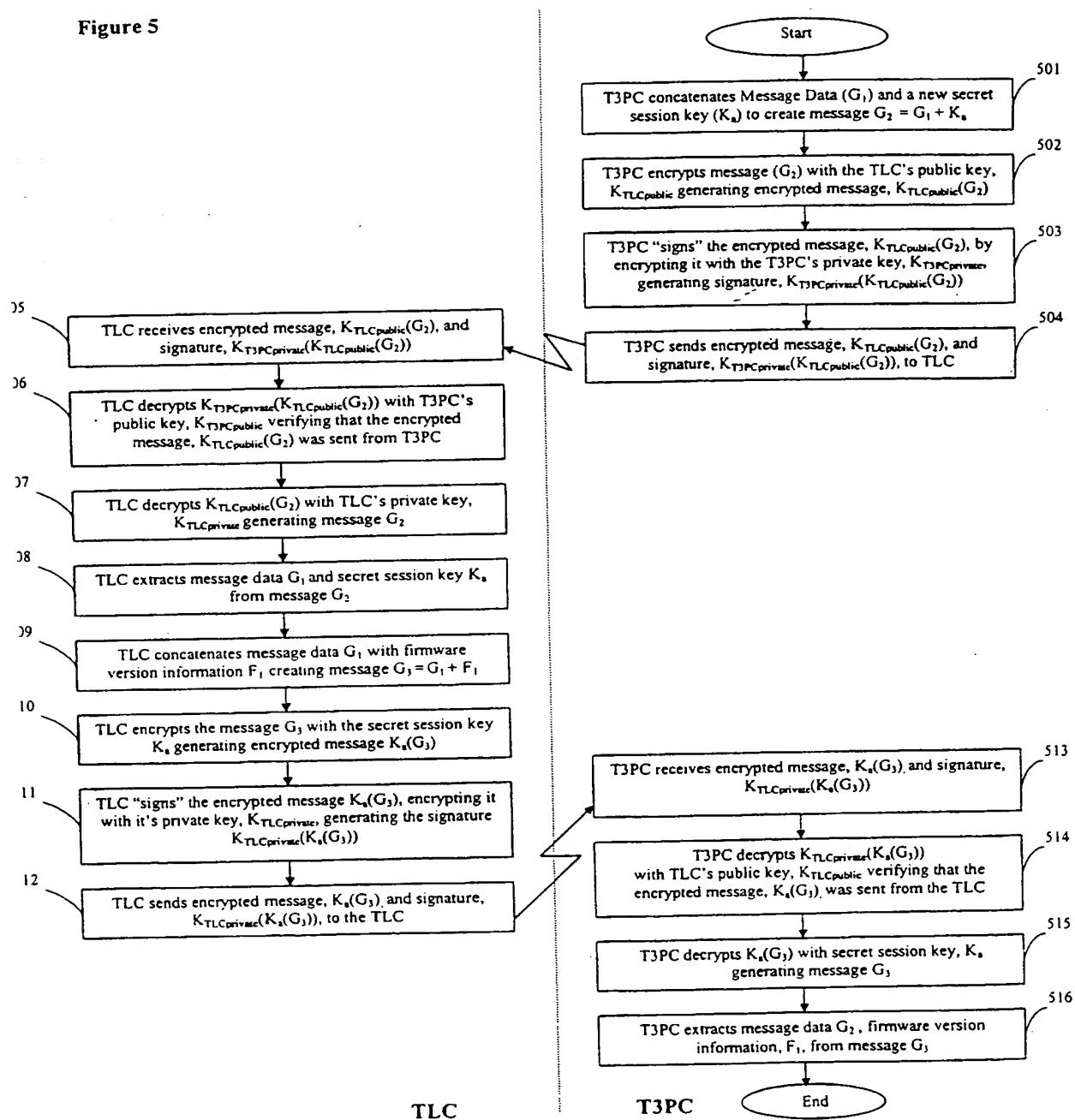
Figure 4

Figure 5



PCT/US00/40168

Figure 6a

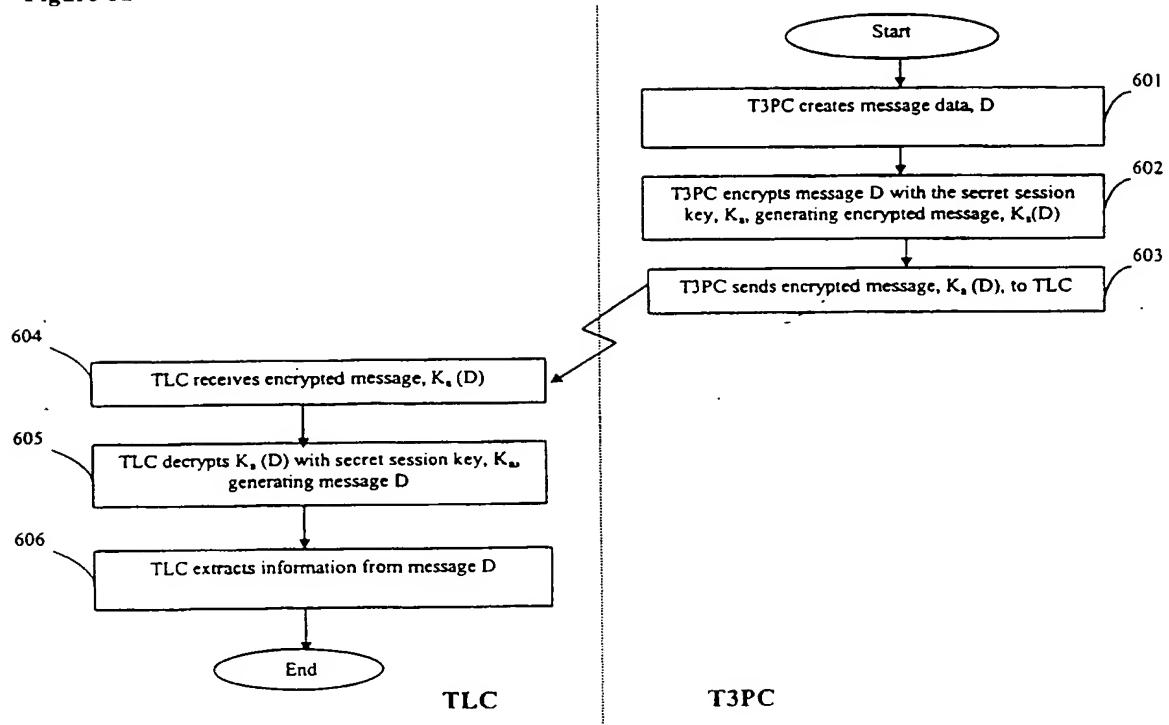


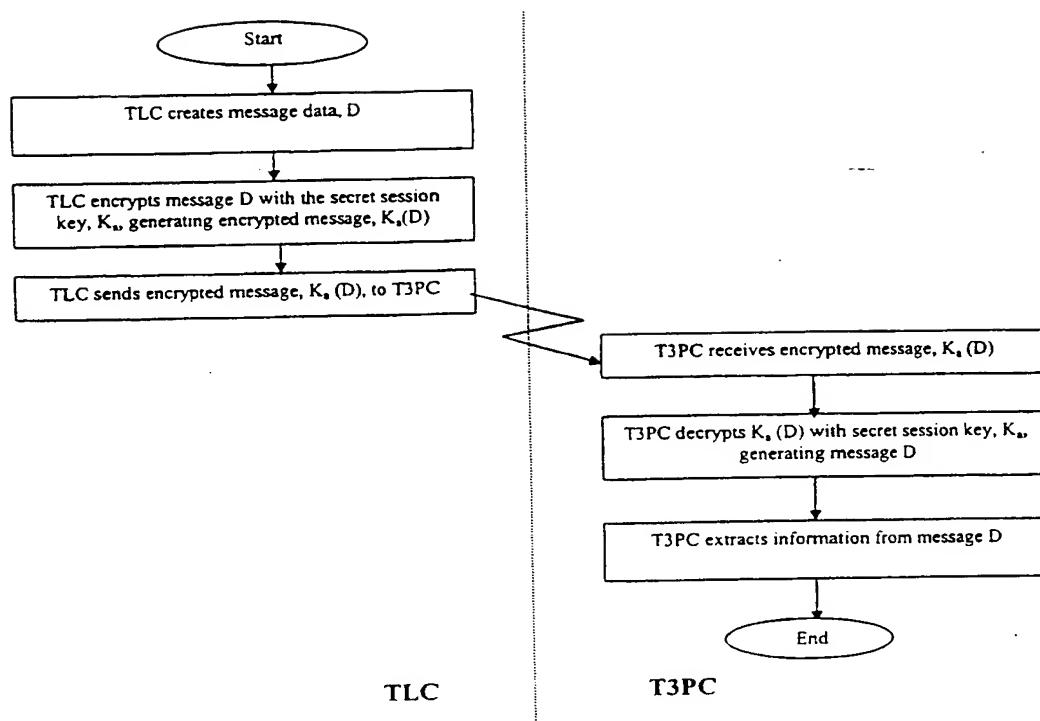
Figure 6b

Figure 7

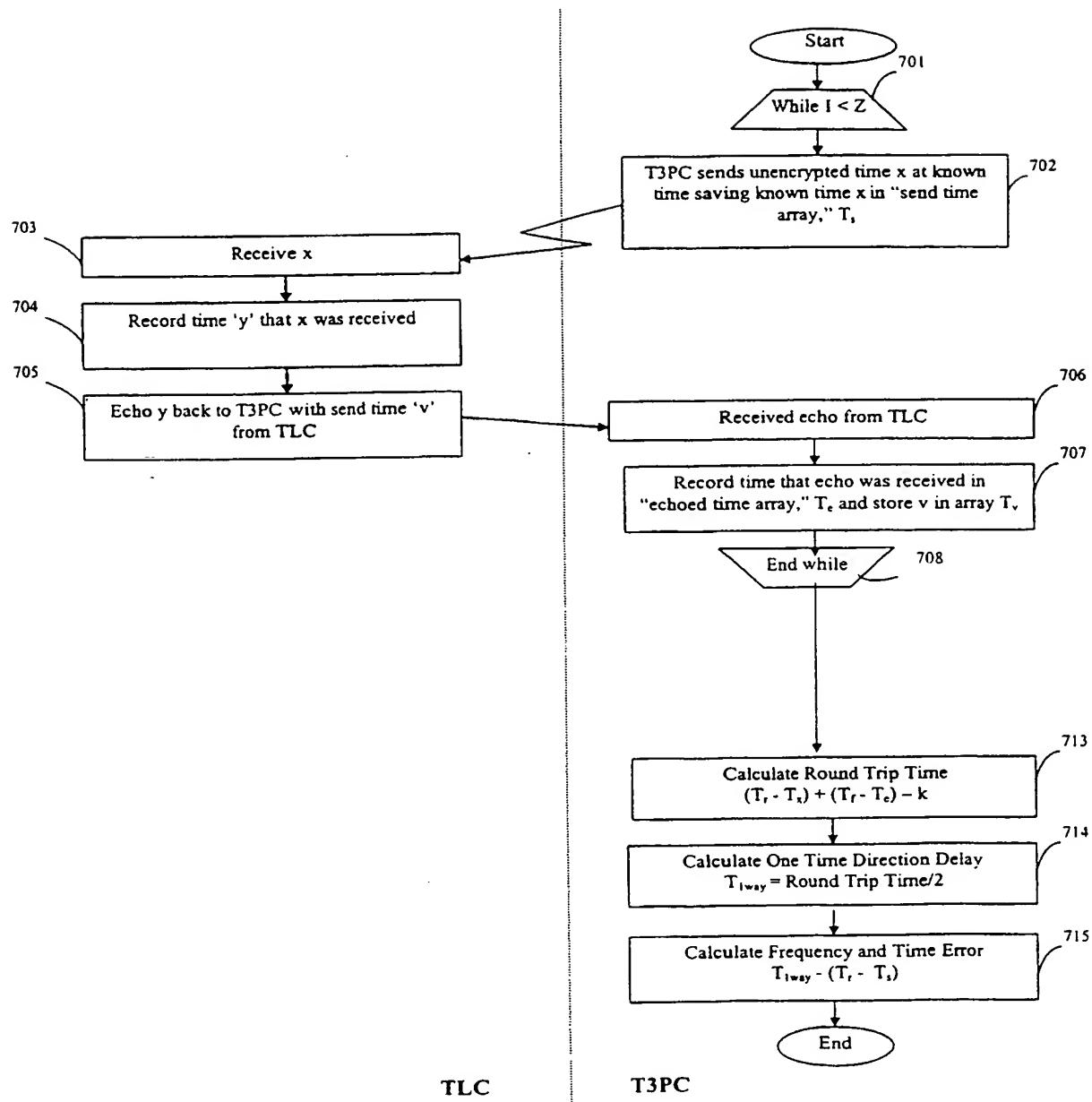


Figure 8

